| Notice of Allowability | Application No. | Applicant(s) |
|---|---|---|
| | 09/328,726 | COLLINS ET AL. |
| | Examiner | Art Unit |
| | Paula W. Klimach | 2135 |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--*

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 03/03/05.
2. ☒ The allowed claim(s) is/are 17-66 and 73-122.
3. ☒ The drawings filed on 26 October 1998 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. ____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: ____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
   1) ☐ hereto or 2) ☐ to Paper No./Mail Date ____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date ____.

   **Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 01/07/2005
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date ____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other ____.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

**EXAMINER'S AMENDMENT**

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with John A. Castellano on 5/2/05. The application has been amended as follows:

17. A <u>processor-implemented</u> method for establishing cryptographic communications, comprising the steps of:

encoding a plaintext message word M to a ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$0 \leq M \leq n-1$,

wherein n is a composite number formed by the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k is an integer greater than 2 and $p_1, p_2, \ldots, P_k$ are distinct random prime numbers, C is a number representative of an encoded form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C, whereby

$C \equiv M^e \pmod{n}$,

and wherein e is a number relatively prime to $(p_1-1), (p_2-1), \ldots$, and $(p_k-1)$; and

decoding said ciphertext word C to a receive message word M', said decoding step being performed using a decryption exponent d that is defined by

$d \equiv e^{-1} \bmod ((p_1 -1)(p_2 -1) \ldots (p_k-1))$,

said decoding step including the further steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{d_1} (\bmod p_1),$$

$$M_2' \equiv C_2^{d_2} (\bmod p_2),$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} (\bmod p_k),$$

wherein

$$C_1 \equiv C(\bmod p_1),$$

$$C_2 \equiv C(\bmod p_2),$$

$$\vdots$$

$$C_k \equiv C(\bmod p_k),$$

$$d_1 \equiv d(\bmod(p_1 - 1)),$$

$$d_2 \equiv d(\bmod(p_2 - 1)), \text{ and}$$

$$\vdots$$

$$d_k \equiv d(\bmod(p_k - 1)),$$

solving said sub-tasks to determine results $M_1', M_2', ..M_k'$, and

combining said results of said sub-tasks to produce said receive message word $M'$, wherein $M' = M$.

18. A processor-implemented method as recited in claim 17 wherein said step of combining said results of said sub-tasks includes a step of performing a recursive combining process to produce said receive message word $M'$.

19. A processor-implemented method as recited in claim 18 wherein said recursive combining process is performed in accordance with

$$Y_i \equiv Y_{i-1} + \left[ (M_i' - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i \right] \bullet w_i \bmod n,$$

wherein $2 \le i \le k$, and

$$M' = Y_k, Y_1 = M_1', and\ w_i = \prod_{j<i} p_j.$$

20. A processor-implemented method as recited in claim 17 wherein said step of combining said results of said sub-tasks includes a step of performing a summation process to produce said receive message word $M'$.

21. A processor-implemented method as recited in claim 20 wherein said summation process is performed in accordance with

$$M' \equiv \sum_{i=1}^{k} M_i'(w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j .$$

28. A processor-implemented method as recited in claim 27 wherein said step of combining said results of said subtasks includes a step of performing a recursive combining process to produce said ciphertext word C.

29. A processor-implemented method as recited in claim 28 wherein said recursive combining process is performed in accordance with

$$Y_i \equiv Y_{i-1} + \left[ (C_i - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i \right] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$C = Y_{k,} Y_1 = C_1, and\ w_i = \prod_{j<i} p_j .$$

30. A processor-implemented method as recited in claim 27 wherein said step of combining said results of said sub-tasks includes a step of performing a summation process to produce said ciphertext word C.

31. A processor-implemented method as recited in claim 30 wherein said summation process is performed in accordance with

$$C \equiv \sum_{i=1}^{k} C_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j \, .$$

32. A cryptographic communications system for establishing communications, comprising:

a communication medium;

a processor ~~encoding means~~ coupled to said communication medium and operative to transform a transmit message word M to a ciphertext word C, and to transmit said ciphertext word C on said medium, wherein .M corresponds to a number representative of a message, and

$$0 \leq M \leq n-1,$$

n being a composite number formed from the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$ wherein k is an integer greater than 2 and $p_1$, $p_2$, ..., $p_k$, are distinct random prime numbers, and wherein the ciphertext word C is a number representative of an encoded form of message word M, said processor being operative to transform said transmit message word M to said ciphertext word C by performing an encoding process comprising the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{e_1} (\bmod p_1),$$

$$C_2 \equiv M_2^{e_2} (\bmod p_2),$$

$$\vdots$$

$$C_k \equiv M_k^{e_k} (\bmod p_k),$$

wherein

$$M_1 \equiv M (\bmod p_1),$$

$$M_2 \equiv M (\bmod p_2),$$

$$\vdots$$

$$M_k \equiv M (\bmod p_k),$$

$$e_1 \equiv e(\bmod (p_1 - 1)),$$

$$e_2 \equiv e(\mathrm{mod}(p_2 - 1)), \text{ and}$$

$$\vdots$$

$$e_k \equiv e(\mathrm{mod}(p_k - 1)),$$

wherein e is a number relatively prime to ($p_1$-1), ($p_2$-1), …, and ($p_k$-1), solving said sub-tasks to determine results $C_1$, $C_2$, … $C_k$, and

combining said results of said sub-tasks to produce said ciphertext word C.

33. A cryptographic communications system as recited in claim 32 wherein said ~~encoding means~~processor is operative to combine said results of said sub-tasks by performing a recursive combining process to produce said ciphertext word C.

34. A cryptographic communications system as recited in claim 33 wherein said ~~encoding means~~processor is operative to perform said recursive combining process in accordance with

$$Y_i \equiv Y_{i-1} + \left[(C_i - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i\right] \bullet w_i \bmod n,$$

wherein $2 \le i \le k$, and

$$C = Y_k, Y_1 = C_1, \text{and } w_i = \prod_{j<i} p_j.$$

35. A cryptographic communications system as recited in claim 32 wherein said ~~encoding means~~processor is operative to combine said results of said sub-tasks by performing a summation process to produce said message word C.

36. A cryptographic communications system as recited in claim 35 wherein said ~~encoding means~~processor is operative to perform said summation process in accordance with

$$C \equiv \sum_{i=1}^{k} C_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \ne i} p_j.$$

37. A processor-implemented method for establishing cryptographic communications, comprising the steps of:

decoding a ciphertext word C to a message word M, wherein M corresponds to a number representative of a message and wherein

$$0 \le M \le n-1$$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and $p_1$, $p_2$, ..., $p_k$ are distinct random prime numbers, C is a number representative of an encoded form of message word M that is encoded by transforming said message word M to said ciphertext word C whereby

$$C \equiv M^e (\text{mod } n),$$

and wherein e is a number relatively prime to $(p_1\text{-}1)$, $(p_2\text{-}1)$, ..., and $(p_k\text{-}1)$;

said decoding step being performed using a decryption exponent d that is defined by

$$d \equiv e^{-1} \text{mod}((p_1-1)(p_2-1)\ldots(p_k-1)),$$

wherein said step of decoding includes the steps of

defining a plurality of k sub-tasks in accordance with

$$M_1 \equiv C_1^{d_1} (\text{mod } p_1),$$

$$M_2 \equiv C_2^{d_2} (\text{mod } p_2),$$

$$\vdots$$

$$M_k \equiv C_k^{d_k} (\text{mod } p_k),$$

wherein

$$C_1 \equiv C (\text{mod } p_1),$$

$$C_2 \equiv C (\text{mod } p_2),$$

$$\vdots$$

$$C_k \equiv C (\text{mod } p_k),$$

$$d_1 \equiv d(\text{mod}(p_1-1)),$$

$$d_2 \equiv d(\text{mod}(p_2-1)), \text{ and}$$

$$\vdots$$

$$d_k \equiv d(\bmod(p_k - 1)),$$

solving said sub-tasks to determine results $M_1$, $M_2$,... $M_k$, and

combining said results of said sub-tasks to produce said message word M.

38. A processor-implemented method as recited in claim 37 wherein said step of combining said results of said sub-tasks includes a step of performing a recursive combining process to produce said message word M.

39. A processor-implemented method as recited in claim 38 wherein said recursive combining process is performed in accordance with

$$Y_i \equiv Y_{i-1} + \left[(M_i - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i\right] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$M' = Y_k, Y_1 = M_1', and\ w_i = \prod_{j<i} p_j.$$

40. A processor-implemented method as recited in claim 37 wherein said step of combining said results of said sub-tasks includes a step of performing a summation process to produce said message word M.

41. A processor-implemented method as recited in claim 40 wherein said summation process is performed in accordance with

$$M \equiv \sum_{i=1}^{k} M_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j.$$

42. A cryptographic communications system for establishing communications, comprising:

a communication medium;

~~decoding means~~a processor communicatively coupled with said communication medium for receiving a ciphertext word C via said medium, and being operative to transform said ciphertext word C to a receive message word M', wherein a message M corresponds to a number representative of a message and wherein,

$$0 \leq M \leq n-1$$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and $p_1$, $p_2$, ..., $p_k$ are distinct random prime numbers, and wherein said ciphertext word C is a number representative of an encoded form of said message word M that is encoded by transforming M to said ciphertext word C whereby,

$$C \equiv M^e \pmod{n},$$

and wherein e is a number relatively prime to $(p_1-1)$, $(p_2-1)$, ..., and $(p_k-1)$;

said ~~decoding means~~processor being operative to perform a decryption process using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1)\ldots(p_k-1)),$$

said decryption process including the steps of

defining a plurality of k sub-tasks in accordance with,

$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d(\bmod(p_1-1)),$$

$$d_2 \equiv d(\bmod(p_2 - 1)), \text{ and}$$

$$\vdots$$

$$d_k \equiv d(\bmod(p_k - 1)),$$

solving said sub-tasks to determine results $M_1', M_2', \ldots M_k'$, and

combining said results of said sub-tasks to produce said receive message word $M'$, wherein $M' = M$.

43. A cryptographic communications system as recited in claim 42 wherein said ~~decoding means~~processor is operative to combine said results of said sub-tasks by performing a recursive combining process to produce said receive message word $M'$.

44. A cryptographic communications system as recited in claim 41 wherein said ~~decoding means~~processor is operative to perform said recursive combining process in accordance with

$$Y_i \equiv Y_{i-1} + \left[(M_i' - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i\right] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$M = Y_k, Y_1 = M_1', and\ w_i = \prod_{j<i} p_j.$$

45. A cryptographic communications system as recited in claim 42 wherein said ~~decoding means~~processor is operative to combine said results of said sub-tasks by performing a summation process to produce said receive message word $M'$.

46. A cryptographic communications system as recited in claim 45 wherein said ~~decoding means~~processor is operative to perform said summation process in accordance with

$$M' \equiv \sum_{i=1}^{k} M_i'(w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j.$$

47. A processor-implemented method for generating a digital signature, comprising the step of:

signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message, and

$$0 \le M \le n-1,$$

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, wherein k is an integer greater than 2 and $p_1$, $p_2$, ..., $p_k$ are distinct random prime numbers, and wherein the signed cipher text word C is a number representative of a signed form of message word M, wherein

$$C \equiv M^d \pmod{n}, \text{ and}$$

wherein said step of signing includes the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{d_1} \pmod{p_1},$$
$$C_2 \equiv M_2^{d_2} \pmod{p_2},$$
$$\vdots$$
$$C_k \equiv M_k^{d_k} \pmod{p_k},$$

wherein

$$M_1 \equiv M \pmod{p_1},$$
$$M_2 \equiv M \pmod{p_2},$$
$$\vdots$$
$$M_k \equiv M \pmod{p_k},$$

$$d_1 \equiv d(\bmod(p_1 - 1)),$$
$$d_2 \equiv d(\bmod(p_2 - 1)), \text{ and}$$
$$\vdots$$
$$d_k \equiv d(\bmod(p_k - 1)),$$

where d id defined by

$d \equiv e^{-1} \bmod((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1))$, and

e is a number relatively prime to ($p_1$-1), ($p_2$-1), ..., and ($p_k$-1), solving said sub-tasks to determine results $C_1, C_2, \ldots C_k$, and

combining said results of said sub-tasks to produce said ciphertext word C.

48. A processor-implemented method as recited in claim 47 wherein said step of combining said results of said sub-asks includes a step of performing a recursive combining process to produce said ciphertext word C.

49. A processor-implemented method as recited in claim 48 wherein said recursive combining process is performed in accordance with

$$Y_i \equiv Y_{i-1} + \left[(C_i - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i\right] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$C = Y_k, Y_1 = C_1, and\ w_i = \prod_{j<i} p_j .$$

50. A processor-implemented method as recited in claim 47 wherein said step of combining said results of said sub-tasks includes a step of performing a summation process to produce said signed ciphertext word C.

51. A processor-implemented method as recited in claim 50 wherein said summation process is performed in accordance with

$$C \equiv \sum_{i=1}^{k} C_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j .$$

52. A digital signature generation system, comprising:

a communication medium;

~~digital signature generating means~~a processor coupled to said communication medium and operative to transform a transmit message word M to a signed ciphertext word C, and to transmit said signed ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$$0 \leq M \leq n-1,$$

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k wherein k is an integer greater than 2 and $p_1$, $p_2$, ..., $p_k$, are distinct random prime numbers, and wherein the signed ciphertext word C is a number representative of a signed form of said message word M, wherein

$$C \equiv M^d (\bmod n),$$

said ~~digital signature generating means~~processor being operative to transform said transmit message word M to said signed ciphertext word C by performing a digital signature generating process comprising the steps of,

defining a plurality of k sub-tasks in accordance with,

$$C_1 \equiv M_1^{d_1} (\bmod p_1),$$
$$C_2 \equiv M_2^{d_2} (\bmod p_2),$$
$$\vdots$$
$$C_k \equiv M_k^{d_k} (\bmod p_k),$$

wherein

$$M_1 \equiv M (\bmod p_1),$$
$$M_2 \equiv M (\bmod p_2),$$
$$\vdots$$
$$M_k \equiv M (\bmod p_k),$$

$$d_1 \equiv d(\bmod(p_1 - 1)),$$
$$d_2 \equiv d(\bmod(p_2 - 1)), \text{ and}$$
$$\vdots$$
$$d_k \equiv d(\bmod(p_k - 1)),$$

where d id defined by

$d \equiv e^{-1} \bmod((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1))$, and

e is a number relatively prime to ($p_1$-1), ($p_2$-1), ..., and ($p_k$-1), solving said sub-tasks to determine results $C_1$, $C_2$, ... $C_k$, and

combining said results of said sub-tasks to produce said ciphertext word C.

53. A digital signature generation system as recited in claim 52 wherein said ~~signature generating means~~ processoris operative to combine said results of said sub-tasks by performing a recursive combining process to produce said signed ciphertext word C.

54. A digital signature generation system as recited in claim 53 wherein said ~~signature generating means~~ processor is operative to perform said recursive combining process in accordance with $Y_i \equiv Y_{i-1} + \left[(M_i' - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i\right] \bullet w_i \bmod n,$

wherein $2 \le i \le k$, and

$C = Y_k, Y_1 = C_1, and\ w_i = \prod_{j<i} p_j$.

55. A digital signature generation system as recited in claim 52 wherein said ~~signature generating means~~ processor is operative to combine said results of said sub-tasks by performing a summation process to produce said signed message word C.

56. A digital signature system as recited in claim 55 wherein said ~~signature generating means~~processor

is operative to perform said summation process in accordance with

$$C \equiv \sum_{i=1}^{k} C_i (w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \ne i} p_j .$$

57. A processor-implemented digital signature process, comprising the steps of:

signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$$0 \leq M \leq n-1$$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and $p_1$, $p_2$, ..., $p_k$ are distinct random prime numbers, C is a number representative of a signed form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C whereby,

$$C = M^d \pmod n,$$

wherein d is defined by

$$d \equiv e^{-1} \bmod((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1)), \text{ and}$$

e is a number relatively prime to $(p_1-1)$, $(p_2-1)$, ..., and $(p_k-1)$; and

verifying said ciphertext word C to a receive message word M' by performing the steps of,.

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{e_1} \pmod{p_1},$$

$$M_2' \equiv C_2^{e_2} \pmod{p_2},$$

$$\vdots$$

$$M_k' \equiv C_k^{e_k} \pmod{p_k},$$

wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv C \pmod{p_k},$$

$$e_1 \equiv e(\bmod(p_1 - 1)),$$

$$e_2 \equiv e(\bmod(p_2 - 1)), \text{ and}$$

$$\vdots$$

$$e_k \equiv e(\bmod(p_k - 1)),$$

solving said sub-tasks to determine results $M_1', M_2', .. M_k'$, and

combining said results of said sub-tasks to produce said receive message word $M'$, wherein $M' = M$.

58. A processor-implemented digital signature process as recited in claim 57 wherein said step of combining said results of said sub-tasks includes a step of performing a recursive combining process to produce said receive message word $M'$.

59. A processor-implemented digital signature process as recited in claim 58 wherein said recursive combining process is performed in accordance with

$$Y_i \equiv Y_{i-1} + \left[ (M_i' - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i \right] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$M' = Y_k, Y_1 = M_1', and\ w_i = \prod_{j<i} p_j .$$

60. A processor-implemented digital signature process as recited in claim 58 wherein said step of combining said results of said sub-tasks includes a step of performing a summation process to produce said receive message word $M'$.

61. A processor-implemented digital signature process as recited in claim 60 wherein said summation process is performed in accordance with

$$M' \equiv \sum_{i=1}^{k} M_i'(w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j .$$

63. A digital signature system as recited in claim 62 wherein said digital signature verification means ~~decoding means~~ is operative to combine said results of said sub-tasks by performing a recursive combining process to produce said receive message word $M'$.

64. A digital signature system as recited in claim 63 wherein said digital signature verification means ~~decoding means~~ is operative to perform said recursive combining process in accordance with

$$Y_i \equiv Y_{i-1} + \left[ (M_i' - Y_{i-1})(w_i^{-1} \bmod p_i) \bmod p_i \right] \bullet w_i \bmod n,$$

wherein $2 \leq i \leq k$, and

$$M' = Y_k, Y_1 = M_1', and\ w_i = \prod_{j<i} p_j .$$

65. A digital signature system as recited in claim 62 wherein said digital signature verification means ~~decoding means~~ is operative combine said results of said sub-tasks by performing a summation process to produce said receive message word $M'$.

66. A digital signature system as recited in claim 65 wherein said digital signature verification means ~~decoding means~~ is operative to perform said summation process accordance with

$$M' \equiv \sum_{i=1}^{k} M_i'(w_i^{-1} \bmod p_i) w_i \bmod n,$$

where

$$w_i = \prod_{j \neq i} p_j .$$

73. A processor-implemented method as recited in claim 17 wherein said step of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of exponentiator units operating substantially simultaneously.

74. A processor-implemented method as recited in claim 17 wherein each of said distinct random prime numbers has the same number of bits.

77. A processor-implemented method as recited in claim 27 wherein said step of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of exponentiator units operating substantially simultaneously.

78. A processor-implemented method as recited in claim 27 wherein each of said distinct random prime numbers has the same number of bits.

81. A processor-implemented method as recited in claim 37 wherein said step of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of exponentiator units operating substantially simultaneously.

82. A processor-implemented method as recited in claim 37 wherein each of said distinct random prime numbers has the same number of bits.

85. A processor-implemented method as recited in claim 47 wherein said step of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of exponentiator units operating substantially simultaneously.

86. A processor-implemented method as recited in claim 47 wherein each of said distinct random prime number has the same numbers of bits.

88. A digital signature generation system as recited in claim 52 wherein each of said distinct random prime numbers has the same number of bits.

90. A digital signature process as recited in claim 57 wherein each of said distinct random prime numbers has the same number of bits.

92. A digital signature system as recited in claim 62 wherein each of said distinct random prime numbers has the same number of bits.

93. A processor-implemented method as recited in claim 17 wherein the plurality of k sub-tasks are performed in parallel.

94. A processor-implemented method as recited in claim 93 wherein said step of combining uses a form of the Chinese Remainder Theorem (CRT).

97. A processor-implemented method as recited in claim 27 wherein the plurality of k sub-tasks are performed in parallel.

98. A processor-implemented method as recited in claim 97 wherein said step of combining uses a form of the Chinese Remainder Theorem (CRT).

101. A processor-implemented method as recited in claim 37 wherein the plurality of k sub-tasks are performed in parallel.

102. A processor-implemented method as recited in claim 101 wherein said step of combining uses a form of the Chinese Remainder Theorem (CRT).

105. A processor-implemented method as recited in claim 47 wherein the plurality of k sub-tasks are performed in parallel.

106. A processor-implemented method as recited in claim 105 wherein said step of combining uses a form of the Chinese Remainder Theorem (CRT).

113. A processor-implemented method for establishing cryptographic communications, comprising the steps of:

encoding a plaintext message word M to a ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$0 \leq M \leq n-1$,

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and $p_1$, $p_2$, ..., $p_k$ are distinct random prime numbers, C is a number representative of an encoded form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C, whereby

$C \equiv M^e \pmod{n}$,

and wherein e is a number relatively prime to $(p_1-1)$, $(p_2-1)$, ..., and $(p_k-1)$; and

decoding said ciphertext word C to a receive message word M', said decoding step being performed using a decryption exponent d that is defined by

$d \equiv e^{-1} \bmod ((p_1 - 1)(p_2 - 1) \ldots (p_k - 1))$,

said decoding step including the further steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{d_1} (\bmod p_1),$$

$$M_2' \equiv C_2^{d_2} (\bmod p_2),$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} (\bmod p_k),$$

wherein

$$C_1 \equiv C (\bmod p_1),$$

$$C_2 \equiv C (\bmod p_2),$$

$$\vdots$$

$$C_k \equiv C (\bmod p_k),$$

$$d_1 \equiv d(\bmod (p_1 - 1)),$$

$$d_2 \equiv d(\bmod (p_2 - 1)), \text{ and}$$

$$\vdots$$

$$d_k \equiv d(\bmod (p_k - 1)),$$

solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results $M_1', M_2', ..M_k'$, and

combining said results of said sub-tasks to produce said receive message word $M'$, wherein $M' = M$.

115. A processor-implemented method for establishing cryptographic communications, comprising the step of:

encoding a plaintext message word M to a ciphertext word C, wherein M corresponds to a number representative of a message, and

$$0 \le M \le n-1$$

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, wherein k is an integer greater than 2 and $p_1$, $p_2$, ..., $p_k$ are distinct random prime numbers, and wherein the ciphertext word C is a number representative of an encoded form of message word M, wherein said step of encoding includes the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{e_1} (\mathrm{mod}\, p_1),$$
$$C_2 \equiv M_2^{e_2} (\mathrm{mod}\, p_2),$$
$$\vdots$$
$$C_k \equiv M_k^{e_k} (\mathrm{mod}\, p_k),$$

wherein

$$M_1 \equiv M (\mathrm{mod}\, p_1),$$
$$M_2 \equiv M (\mathrm{mod}\, p_2),$$
$$\vdots$$
$$M_k \equiv M (\mathrm{mod}\, p_k),$$

$$e_1 \equiv e(\mathrm{mod}(p_1 - 1)),$$
$$e_2 \equiv e(\mathrm{mod}(p_2 - 1)), \text{ and}$$

$$\vdots$$

$$e_k \equiv e(\mathrm{mod}(p_k - 1)),$$

wherein e is a number relatively prime to ($p_1$-1), ($p_2$-1), ..., and ($p_k$-1), solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results $C_1$, $C_2$, ... $C_k$, and

combining said results of said sub-tasks to produce said ciphertext word C.

116. A cryptographic communications system for establishing communications, comprising:

a communication medium;

~~encoding means~~processor coupled to said communication medium and operative to transform a transmit message word M to a ciphertext word C, and to transmit said ciphertext word C on said medium, wherein .M corresponds to a number representative of a message, and

$$0 \leq M \leq n-1,$$

n being a composite number formed from the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$ wherein k is an integer greater than 2 and $p_1$, $p_2$, ..., $p_k$, are distinct random prime numbers, and wherein the ciphertext word C is a number representative of an encoded form of message word M, said ~~encoding means~~processor being operative to transform said transmit message word M to said ciphertext word C by performing an encoding process comprising the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{e_1}(\mathrm{mod}\, p_1),$$

$$C_2 \equiv M_2^{e_2}(\mathrm{mod}\, p_2),$$

$$\vdots$$

$$C_k \equiv M_k^{e_k}(\mathrm{mod}\, p_k),$$

wherein

$$M_1 \equiv M(\mathrm{mod}\, p_1),$$

$$M_2 \equiv M(\mathrm{mod}\, p_2),$$

$$\vdots$$

$$M_k \equiv M(\mathrm{mod}\, p_k),$$

$$e_1 \equiv e(\mathrm{mod}(p_1 - 1)),$$

$$e_2 \equiv e(\mathrm{mod}(p_2 - 1)), \text{ and}$$

$$\vdots$$

$$e_k \equiv e(\mathrm{mod}(p_k - 1)),$$

wherein e is a number relatively prime to $(p_1\text{-}1)$, $(p_2\text{-}1)$, …, and $(p_k\text{-}1)$, solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results $C_1$, $C_2$, … $C_k$, and

combining said results of said sub-tasks to produce said ciphertext word C.

117. A processor-implemented method for establishing cryptographic communications, comprising the steps of:

decoding a ciphertext word C to a message word M, wherein M corresponds to a number representative of a message and wherein

$$0 \le M \le n-1$$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and $p_1$, $p_2$, …, $p_k$ are distinct random prime numbers, C is a number representative of an encoded form of message word M that is encoded by transforming said message word M to said ciphertext word C whereby

$C \equiv M^e (\mathrm{mod}\ n)$,

and wherein e is a number relatively prime to $(p_1\text{-}1)$, $(p_2\text{-}1)$, ..., and $(p_k\text{-}1)$;

said decoding step being performed using a decryption exponent d that is defined by

$$d \equiv e^{-1} \mathrm{mod}((p_1 - 1)(p_2 - 1)\ldots(p_k - 1)),$$

wherein said step of decoding includes the steps of

defining a plurality of k sub-tasks in accordance with

$$M_1 \equiv C_1^{d_1} (\mathrm{mod}\, p_1),$$

$$M_2 \equiv C_2^{d_2} (\mathrm{mod}\, p_2),$$

$$\vdots$$

$$M_k \equiv C_k^{d_k} (\mathrm{mod}\, p_k),$$

wherein

$$C_1 \equiv C(\text{mod}\, p_1),$$
$$C_2 \equiv C(\text{mod}\, p_2),$$
$$\vdots$$
$$C_k \equiv C(\text{mod}\, p_k),$$

$$d_1 \equiv d(\text{mod}(p_1 - 1)),$$
$$d_2 \equiv d(\text{mod}(p_2 - 1)), \text{ and}$$
$$\vdots$$
$$d_k \equiv d(\text{mod}(p_k - 1)),$$

solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results $M_1$, $M_2$,... $M_k$, and

combining said results of said sub-tasks to produce said message word M.

118. A cryptographic communications system for establishing communications, comprising:

a communication medium;

~~decoding means~~processor communicatively coupled with said communication medium for receiving a ciphertext word C via said medium, and being operative to transform said ciphertext word C to a receive message word M', wherein a message M corresponds to a number representative of a message and wherein,

$0 \leq M \leq n-1$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, k is an integer greater than 2 and $p_1$, $p_2$, ..., $p_k$ are distinct random prime numbers, and wherein said ciphertext word C is a number representative of an encoded form of said message word M that is encoded by transforming M to said ciphertext word C whereby,

$C \equiv M^e \text{ (mod n)},$

and wherein e is a number relatively prime to ($p_1$-1), ($p_2$-1), ..., and ($p_k$-1);

said ~~decoding means~~ processor being operative to perform a decryption process using a decryption exponent d that is defined by

$$d \equiv e^{-1} \bmod((p_1 - 1)(p_2 - 1)\ldots(p_k - 1)),$$

said decryption process including the steps of

defining a plurality of k sub-tasks in accordance with,

$$M_1' \equiv C_1^{d_1} (\bmod p_1),$$

$$M_2' \equiv C_2^{d_2} (\bmod p_2),$$

$$\vdots$$

$$M_k' \equiv C_k^{d_k} (\bmod p_k),$$

wherein

$$C_1 \equiv C(\bmod p_1),$$

$$C_2 \equiv C(\bmod p_2),$$

$$\vdots$$

$$C_k \equiv C(\bmod p_k),$$

$$d_1 \equiv d(\bmod(p_1 - 1)),$$

$$d_2 \equiv d(\bmod(p_2 - 1)), \text{ and}$$

$$\vdots$$

$$d_k \equiv d(\bmod(p_k - 1)),$$

solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results $M_1', M_2', ..M_k'$, and

combining said results of said sub-tasks to produce said receive message word $M'$, wherein $M' = M$.

119. A processor-implemented method for generating a digital signature, comprising the step of:

signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message, and

$0 \leq M \leq n-1$,

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, wherein k is an integer greater than 2 and $p_1$, $p_2$, …, $p_k$ are distinct random prime numbers, and wherein the signed cipher-text word C is a number representative of a signed form of message word M, wherein

$C \equiv M^d (\bmod n)$, and

wherein said step of signing includes the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{d_1} (\bmod p_1),$$
$$C_2 \equiv M_2^{d_2} (\bmod p_2),$$
$$\vdots$$
$$C_k \equiv M_k^{d_k} (\bmod p_k),$$

wherein

$$M_1 \equiv M (\bmod p_1),$$
$$M_2 \equiv M (\bmod p_2),$$
$$\vdots$$
$$M_k \equiv M (\bmod p_k),$$

$$d_1 \equiv d(\bmod(p_1 - 1)),$$
$$d_2 \equiv d(\bmod(p_2 - 1)), \text{ and}$$
$$\vdots$$
$$d_k \equiv d(\bmod(p_k - 1)),$$

where d id defined by

$d \equiv e^{-1} \bmod((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1))$, and

e is a number relatively prime to $(p_1\text{-}1)$, $(p_2\text{-}1)$, ..., and $(p_k\text{-}1)$, solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results $C_1$, $C_2$, ... $C_k$, and

combining said results of said sub-tasks to produce said ciphertext word C.

120. A digital signature generation system, comprising:

a communication medium;

~~digital signature generating means~~ a processor coupled to said communication medium and operative to transform a transmit message word M to a signed ciphertext word C, and to transmit said signed ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$$0 \le M \le n-1,$$

n being a composite number formed from the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k wherein k is an integer greater than 2 and $p_1$, $p_2$, ..., $p_k$, are distinct random prime numbers, and wherein the signed ciphertext word C is a number representative of a signed form of said message word M, wherein

$$C \equiv M^d (\bmod n),$$

said ~~digital signature generation means~~ processor being operative to transform said transmit message word M to said signed ciphertext word C by performing a digital signature generating process comprising the steps of,

defining a plurality of k sub-tasks in accordance with,

$$C_1 \equiv M_1^{d_1} (\bmod p_1),$$
$$C_2 \equiv M_2^{d_2} (\bmod p_2),$$
$$\vdots$$
$$C_k \equiv M_k^{d_k} (\bmod p_k),$$

wherein

$$M_1 \equiv M (\bmod p_1),$$
$$M_2 \equiv M (\bmod p_2),$$
$$\vdots$$

$$M_k \equiv M(\text{mod}\, p_k),$$

$$d_1 \equiv d(\text{mod}(p_1 - 1)),$$

$$d_2 \equiv d(\text{mod}(p_2 - 1)), \text{ and}$$

$$\vdots$$

$$d_k \equiv d(\text{mod}(p_k - 1)),$$

where d id defined by

$d \equiv e^{-1} \text{mod}((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1))$, and

e is a number relatively prime to ($p_1$-1), ($p_2$-1), ..., and ($p_k$-1), solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results $C_1$, $C_2$, ... $C_k$, and

combining said results of said sub-tasks to produce said ciphertext word C.

121. A processor-implemented digital signature process, comprising the steps of:

signing a plaintext message word M to create a signed ciphertext word C, wherein M corresponds to a number representative of a message and wherein

$0 \le M \le n - 1$

wherein n is a composite number formed by the product of $p_1 \bullet p_2 \bullet \ldots \bullet p_k$, k is an integer greater than 2 and $p_1$, $p_2$, ..., $p_k$ are distinct random prime numbers, C is a number representative of a signed form of message word M, and wherein said encoding step comprises transforming said message word M to said ciphertext word C whereby,

$C = M^d \text{ (mod n)}$,

wherein d is defined by

$d \equiv e^{-1} \text{mod}((p_1 - 1) \bullet (p_2 - 1) \bullet \ldots \bullet (p_k - 1))$, and

e is a number relatively prime to ($p_1$-1), ($p_2$-1), ..., and ($p_k$-1); and

verifying said ciphertext word C to a receive message word M' by performing the steps of,

defining a plurality of k sub-tasks in accordance with

$$M_1' \equiv C_1^{e_1} (\bmod\, p_1),$$

$$M_2' \equiv C_2^{e_2} (\bmod\, p_2),$$

$$\vdots$$

$$M_k' \equiv C_k^{e_k} (\bmod\, p_k),$$

wherein

$$C_1 \equiv C(\bmod\, p_1),$$

$$C_2 \equiv C(\bmod\, p_2),$$

$$\vdots$$

$$C_k \equiv C(\bmod\, p_k),$$

$$e_1 \equiv e(\bmod(p_1 - 1)),$$

$$e_2 \equiv e(\bmod(p_2 - 1)), \text{ and}$$

$$\vdots$$

$$e_k \equiv e(\bmod(p_k - 1)),$$

solving said sub-tasks in parallel using a form of the Chinese Remainder Theorem wherein each sub-task is a Chinese Remainder Theorem sub-problem to determine results $M_1', M_2', \ldots M_k'$, and

combining said results of said sub-tasks to produce said receive message word $M'$, wherein $M' = M$.

## *Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Friday, May 13, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100